In the Claims:

This listing of claims replaces all prior versions and listing of claims in the application.

1. (Previously Presented) A cryptographic device comprising:

a cryptographic module and a communications module removably coupled thereto;

said cryptographic module comprising

a first housing,

a user Local Area Network (LAN) interface carried by said first housing,

a cryptographic processor carried by said first housing and coupled to said user LAN interface, and

a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing;

said communications module comprising

a second housing, and

a network wireless LAN interface carried by said second housing, coupled to said cryptographic processor and switchable between wireless LAN modes.

2. (Original) The cryptographic device of Claim 1 wherein said network wireless LAN interface circuit is switchable to one of an access point (AP) mode, an infrastructure mode, and an ad-hoc mode.

3. (Original) The cryptographic device of Claim 1

wherein said cryptographic module further comprises a first connector carried by said first housing and coupled to said cryptographic processor; wherein said communications module further comprises a second connector carried by said second housing and connected to said network wireless LAN interface, said second connector being removably mateable with said first connector of said cryptographic module.

4. (Original) The cryptographic device of Claim 1 wherein said user LAN interface comprises an Ethernet interface.

5. (Original) The cryptographic device of Claim 1 further comprising a power circuit carried by said first housing and powering said cryptographic processor, said user LAN interface, and said network LAN interface.

6. (Original) The cryptographic device of Claim 1 wherein said cryptographic processor implements an encryption algorithm to provide a predetermined security level.

7. (Original) The cryptographic device of Claim 1 wherein said cryptographic processor comprises:

a host network processor coupled to said user LAN interface; and

a cryptography circuit coupled to said host network processor.

8. (Original) The cryptographic device of Claim 7

wherein said cryptographic processor further comprises:

an encrypted data buffer circuit coupled between said user LAN interface and said cryptography circuit; and

an unencrypted data buffer circuit coupled between said cryptography circuit and said network LAN interface.

9. (Cancelled).

10. (Previously Presented) The cryptographic device of Claim 1 wherein said tamper circuit comprises at least one conductor substantially surrounding said cryptographic processor, and wherein said cryptographic processor is disabled based upon a break in said at least one conductor.

11. (Previously Presented) A cryptographic device comprising:

a cryptographic module and a communications module removably coupled thereto;

said cryptographic module comprising

a first housing,

a user Local Area Network (LAN) interface carried by said first housing,

a cryptographic processor carried by said first housing and coupled to said user LAN interface, and

a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing;

said communications module comprising a second housing and a network wireless LAN interface carried by said second

housing;

said communications module comprising a predetermined one from among a plurality of interchangeable communications modules, and said network wireless LAN interfaces of said plurality of interchangeable communications modules each operating using a different wireless LAN mode.

12. (Original) The cryptographic device of Claim 11 wherein the different wireless LAN modes comprise an access point (AP) mode, an infrastructure mode, and an ad-hoc mode.

13. (Original) The cryptographic device of Claim 11 wherein said cryptographic module further comprises a first connector carried by said first housing and coupled to said cryptographic processor; wherein said communications module further comprises a second connector carried by said second housing and connected to said network wireless LAN interface, said second connector being removably mateable with said first connector of said cryptographic module.

14. (Original) The cryptographic device of Claim 11 wherein said user LAN interface comprises an Ethernet interface.

15. (Original) The cryptographic device of Claim 11 further comprising a power circuit carried by said first housing and powering said cryptographic processor, said user LAN interface, and said network LAN interface.

16. (Original) The cryptographic device of Claim 11 wherein said cryptographic processor implements an encryption algorithm to provide a predetermined security level.

17. (Original) The cryptographic device of Claim 11 wherein said cryptographic processor comprises:

a host network processor coupled to said user LAN interface; and

a cryptography circuit coupled to said host network processor.

18. (Original) The cryptographic device of Claim 17 wherein said cryptographic processor further comprises:

an encrypted data buffer circuit coupled between said user LAN interface and said cryptography circuit; and

an unencrypted data buffer circuit coupled between said cryptography circuit and said network LAN interface.

19. (Cancelled).

20. (Previously Presented) The cryptographic device of Claim 11 wherein said tamper circuit comprises at least one conductor substantially surrounding said cryptographic processor, and wherein said cryptographic processor is disabled based upon a break in said at least one conductor.

21. (Previously Presented) A communications method comprising:

coupling a cryptographic module to a Local Area Network (LAN) device, the cryptographic module comprising a first housing, a user LAN interface carried by the first housing, a cryptographic processor carried by the first housing and coupled to the user LAN interface, and a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing;

providing a communications module comprising a second housing and a network wireless LAN interface carried by the second housing and removably coupled to the cryptographic module; and

switching the network wireless LAN interface between wireless LAN modes, and using the network wireless LAN to communicate with a wireless LAN.

22. (Original) The method of Claim 21 wherein switching comprises switching the network wireless LAN interface circuit to one of an access point (AP) mode, an infrastructure mode, and an ad-hoc mode.

23. (Original) The method of Claim 21 wherein the cryptographic module further comprises a first connector carried by the first housing and coupled to the cryptographic processor; wherein the communications module further comprises a second connector carried by the second housing and connected to the network wireless LAN interface; and wherein removably coupling comprises removably mating the second connector to the first connector.

24. (Original) The method of Claim 21 wherein the user LAN interface comprises an Ethernet interface.

25. (Previously Presented) A communications method comprising:

coupling a cryptographic module to a Local Area Network (LAN) device, the cryptographic module comprising a first housing, a user Local Area Network (LAN) interface carried by the first housing, and a cryptographic processor carried by the first housing and coupled to the user LAN interface, and a tamper circuit for disabling the cryptographic processor based upon tampering with the first housing;

coupling the user LAN interface to a LAN device;

removably coupling one of a plurality of communications modules to the cryptographic module, the communications module comprising a second housing and a network wireless LAN interface carried by the second housing, and the network wireless LAN interfaces of the plurality of interchangeable communications modules each operating in a different wireless LAN mode; and

using the removably coupled communications module to communicate with a LAN.

26. (Original) The method of Claim 25 wherein the different wireless LAN modes comprise an access point (AP) mode, an infrastructure mode, and an ad-hoc mode.

27. (Original) The method of Claim 25 wherein the

cryptographic module further comprises a first connector carried by the first housing and coupled to the cryptographic processor; wherein the communications module further comprises a second connector carried by the second housing and connected to the network wireless LAN interface; and wherein removably connecting comprises removably mating the second connector with the first connector of the cryptographic module.

28. (Original) The method of Claim 25 wherein the user LAN interface comprises an Ethernet interface.

29. (Previously Presented) A communications system comprising:

a plurality of Local Area Network (LAN) devices coupled together to define a wireless LAN, and a cryptographic device coupled to at least one of said LAN devices;

said cryptographic device comprising a cryptographic module coupled to said at least one LAN device, and a communications module removably coupled to said cryptographic module;

said cryptographic module comprising

a first housing,

a user LAN interface carried by said first housing,

a cryptographic processor carried by said first housing and coupled to said user LAN interface, and

a tamper circuit for disabling said cryptographic processor based upon tampering with said first housing;

said communications module comprising

a second housing, and

a network wireless LAN interface carried by said second housing, coupled to said cryptographic processor and switchable between wireless LAN modes.

30. (Original) The communications system of Claim 29 wherein said network wireless LAN interface circuit is switchable to one of an access point (AP) mode, an infrastructure mode, and an ad-hoc mode.

31. (Original) The communications system of Claim 29 wherein said cryptographic module further comprises a first connector carried by said first housing and coupled to said cryptographic processor; wherein said communications module further comprises a second connector carried by said second housing and connected to said network wireless LAN interface, said second connector being removably mateable with said first connector of said cryptographic module.

32. (Original) The communications system of Claim 29 wherein said user LAN interface comprises an Ethernet interface.

33. (Original) The communications system of Claim 29 further comprising a power circuit carried by said first housing and powering said cryptographic processor, said user LAN interface, and said network LAN interface.

34. (Original) The communications system of Claim 29 wherein said cryptographic processor implements an encryption algorithm to provide a predetermined security level.

35. (Original) The communications system of Claim 29 wherein said cryptographic processor comprises:

a host network processor coupled to said user LAN interface; and

a cryptography circuit coupled to said host network processor.

36. (Original) The communications system of Claim 35 wherein said cryptographic processor further comprises:

an encrypted data buffer circuit coupled between said user LAN interface and said cryptography circuit; and

an unencrypted data buffer circuit coupled between said cryptography circuit and said network LAN interface.

37. (Previously Presented) The cryptographic device according to Claim 1 wherein said user LAN comprises a plurality of different connectors for coupling the cryptographic module to different network devices.

38. (Previously Presented) The cryptographic device according to Claim 10 wherein said user LAN comprises a plurality of different connectors for coupling the cryptographic module to different network devices.